DEPARTMENT OF STATE

FY 2008
PRIVACY IMPACT ASSESSMENT
WebPASS Explorer
FY 2008 Quarter 2

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy
E-mail: pia@state.gov

IT Project Name/Component System: WebPASS Explorer

NOTE: WebPASS Explorer contains 15 applications, the user-interface front end "parent" Explorer and 14 "child" administrative applications with various sponsors in different areas of the Department.

Subordinate applications are:

(1) Dashboard;
(2) eAllowances;
(3) eServices;
(4) Explorer;
(5) Expendable Supplies;
(6) Generic Service Request (GSR);
(7) International Cooperative Administrative Support Services (ICASS);
(8) New Embassy Compound (NEC);
(9) Pharmacy Inventory System (RxIS);
(10) Post Personnel (PS);
(11) Procurement;
(12) Real Property Application (RPA);
(13) Vehicle Registration and Maintenance (VRM);
(14) Visitor Management (VM); and
(15) Work Orders for Windows (WOW)

A. CONTACT INFORMATION

Who is the Agency Privacy Coordinator who is conducting this assessment?

Ms. Margaret Grafeld, Director
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services

B. GENERAL INFORMATION ABOUT THE SYSTEM/APPLICATION

(1) Does this system collect, maintain or disseminate personally identifiable information (PII) about individual members of the public?**

YES X NO___

If the above answer is YES, please complete the survey in its entirety. If NO, complete the certification page and submit the PIA to the following e-mail address: pia@state.gov.

(2) Does a Privacy Act system of records already exist?

YES X NO___

If yes, please provide the following:
System Name:
Medical Records ; Number STATE-24

If no, a Privacy system of records description will need to be created for this data.

(3) What is the purpose of the system/application?

[NOTE: The only component of WebPASS Explorer that retains information about individual members of the public is the Pharmacy Inventory System (RxIS). All responses will address RxIS specifically rather than the entire program suite.]

The Prescription Inventory System is used by health units to track patients' medical history, including medications to which they are allergic. The system also catalogs all medications at post, their formulations and stock details. Prior to the development of this system, Foreign Service health care professionals used a paper-based process to create and track medications, maintaining written records of destroyed and controlled items, and creating and tracking purchase orders with paper and email. This made compiling reports, and responding to medicine recalls difficult, as sorting through the paper records was slow and tedious.

(4) What legal authority authorizes the purchase or development of this system/application?

22 U.S.C. 911, 912; 22 U.S.C. 1156-1159; 42 U.S.C. 4561; 21 U.S.C. 1180; 22 U.S.C. 3926; and 5 U.S.C. 301

C. DATA IN THE SYSTEM:

1) What categories of individuals are covered in the system?

The system maintains data about employees and their families, specifically prescribed medication, allergies and related information.

2) What are the sources of the information in the system?

a. Who/what is the source of the information?

The employee or employee's family member

b. What type of information is collected from the source of the information?

Patient name; gender; relationship to the employee; name of related employee; agency; interoffice address; work phone; home phone; allergies; current medications; date started on medication; date finished with medication; medication quantity; medication lot batch; number of refills; expiration date; prescriber; and dispenser. The system also maintains records of system use, including user ID, and date and time of system access.

3) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

N/A

b. How will data be checked for completeness?

The medical professional user will verify accuracy and completeness.

c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).

The medical professional user will verify data currency.

D. <u>INTENDED USE OF THE DATA:</u>

1) Will the use of the data be both relevant and necessary to the purpose for which the system is being designed?

Applications Development division personnel worked with the Office of Medical Services' Medical Informatics Branch to establish requirements for this application, and to identify data relevant and necessary for pharmacy management.

RxIS automates the processes described in the Office of Medical Services' Clinical Bulletin #4, "Storage & Dispensing Medications," available at https://med.state.gov/staff/admin_bulletin/clinic/docs/Clinical_Bulletin4.pdf

2) Will new data or previously unavailable personal data be created through derived data or aggregation of data collected, and how will it be maintained and filed?

As new requirements emerge, the application can be modified to include new data. There is no data derivation or aggregation in RxIS.

3) Will the system make determinations about DOS employees or members of the public that would not be possible without the new data?

The system enables tracking patient medication administration.

4) Will the new data be placed in the individual's record?

Medications are tracked by patient name.

5) How will the new data be verified for relevance and accuracy?

The medical professional user will verify data relevance and accuracy.

6) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved by patient name, inventory item or vendor; *ad hoc* queries may also be used. Procedures for use are described in the RxIS User Manual, available at OpenNet http://pass.irm.state.gov/index.cfm?Page=Download%20File&App=14&Cat=11&FileID=1038

7) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

There is a Patient Information report, which lists all the data identified in the response to question C-2-b above. This report is only available to authorized users. Users may generate *ad hoc* reports of their own design.

E. <u>MAINTENANCE OF DATA & ADMINISTRATIVE CONTROLS:</u>

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

Application design maintains consistent use of the system and data. As described above, RxIS automates the processes described in the Office of Medical Services' Clinical Bulletin #4, "Storage & Dispensing Medications," available at https://med.state.gov/staff/admin_bulletin/clinic/docs/Clinical_Bulletin4.pdf

2) What are the retention periods of data in this system?

Medical Offices with Foreign Service medical personnel should ensure that employee/dependant pharmacy information is forwarded to M/MED for inclusion in original case files and forwarded to the employee's new post. Posts without Foreign Service medical personnel, and posts where the employee is being transferred back to the Department, should retain patient data for six years after the date of the last papers in the file. After which point, they may be destroyed in accordance with Foreign Records Disposition Schedule Chapter 06, "Health and Medical Records," Section B-06-000-02a.

Data about medical supplies should be blocked annually and destroyed when three years old, as stated in Section B-06-000-01a.

3) **What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?**

As stated in the answer to question E2, patient data is either forwarded to M/MED or retained for six years, depending on whether Foreign Service medical personnel are at post; medical supply data is retained for three years. RxIS reports are intended for the convenience of the medical professional RxIS user and should be stored in accordance with Sensitive but Unclassified information. Record retention procedures are available on OpenNet at http://infoaccess.state.gov; RxIS procedures follow the processes described in the Office of Medical Services' Clinical Bulletin #4, "Storage & Dispensing Medications," available at https://med.state.gov/staff/admin_bulletin/clinic/docs/Clinical_Bulletin4.pdf

4) **Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?**

No.

5) **How does the use of this technology affect public/employee privacy and does it restrict access to the system?**

Users must be granted access to the system before they can log in; users also must agree to an Access and Usage Acknowledgement.

6) **If this system provides the capability to identify, locate, and monitor individuals, what kinds of information are collected as a function of the monitoring of individuals and what controls are used to prevent unauthorized monitoring?**

The system monitors patient medication administration; only authorized individuals are granted access to the system. The system also maintains date and time information regarding user access.

7) **If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.**

Modification of the system should have no impact on the Privacy Act System of Records Notice; should this occur, the notice will be amended accordingly.

8) **Are there forms associated with the system? YES ___ NO X**

If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

Medical professionals at post and system administrators.

2) What are the criteria for gaining access to the system? Are criteria, procedures, controls, and responsibilities regarding access documented?

Access procedures are documented in the User Manual, at OpenNet http://pass.irm.state.gov/index.cfm?Page=Download%20File&App=14&Cat=11&FileID=1038.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Medical professional users have access to all data on the system; user access is granted by the system administrator. RxIS may be configured by the system administrator to restrict user access to patient data and the reports menu as is deemed appropriate. Given the limited medical staff at posts, it is very often necessary to provide the user with access to the entire system.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those already having access? (Please list processes and training materials)

System administrators do not grant access to persons without a business need to access application data.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Locally employed persons may support the Medical Office according to standard Department procedures. Rules of Behavior are addressed with the Access and Usage Acknowledgement.

6) Will other systems share data or have access to the data in the system? If yes, who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

The medical professional users have responsibility for protecting the data and maintaining security awareness according to standard Department procedures. The Information Management Officer (IMO) is responsible for backups and data recovery.

7) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)? If so, how will the data be used by the other agency?

No.

8) Who is responsible for assuring proper use of the SHARED data?

Not applicable.